

(ii) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;

(iii) Capacity to maintain safe navigation and emergency response;

(iv) Cargo, particularly dangerous goods or hazardous substances;

(v) Vessel stores;

(vi) Any vessel security communication and surveillance systems; and

(vii) Any other vessel security systems, if any.

(4) The VSA must account for any vulnerabilities in the following areas:

(i) Conflicts between safety and security measures;

(ii) Conflicts between vessel duties and security assignments;

(iii) The impact of watch-keeping duties and risk of fatigue on vessel personnel alertness and performance;

(iv) Security training deficiencies; and

(v) Security equipment and systems, including communication systems.

(5) The VSA must discuss and evaluate key vessel measures and operations, including:

(i) Ensuring performance of all security duties;

(ii) Controlling access to the vessel, through the use of identification systems or otherwise;

(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);

(iv) Supervising the handling of cargo and the delivery of vessel stores;

(v) Monitoring restricted areas to ensure that only authorized persons have access;

(vi) Monitoring deck areas and areas surrounding the vessel; and

(vii) The ready availability of security communications, information, and equipment.

(6) The VSA must be documented and the VSA report retained by the vessel owner or operator with the VSP. The VSA and VSP must be protected from unauthorized access or disclosure.

§§ 104.310 Submission requirements.

(a) A completed Vessel Security Assessment (VSA) report must be submitted with the Vessel Security Plan (VSP) required in §104.410 of this part.

(b) A vessel owner or operator may generate and submit a report that contains the VSA for more than one vessel subject to this part, to the extent that they share similarities in physical characteristics and operations.

Subpart D—Vessel Security Plan (VSP)

§ 104.400 General.

(a) The Company Security Officer (CSO) must ensure a Vessel Security Plan (VSP) is developed and implemented for each vessel. The VSP:

(1) Must identify the CSO and VSO by name or position and provide 24-hour contact information;

(2) Must be written in English;

(3) Must address each vulnerability identified in the Vessel Security Assessment (VSA);

(4) Must describe security measures for each MARSEC Level;

(5) Must state the Master's authority as described in §104.205; and

(6) May cover more than one vessel to the extent that they share similarities in physical characteristics and operations, if authorized and approved by the Commanding Officer, Marine Safety Center.

(b) Except for foreign vessels that have on board a valid International Ship Security Certificate (ISSC) that attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, part A (Incorporated by reference, see §101.115 of this subchapter), and having taken into account the relevant provisions in the ISPS Code, part B, the VSP must be submitted for approval to the Commanding Officer, Marine Safety Center (MSC), 400 Seventh Street, SW., Room 6302, Nassif Building, Washington, DC 20590-0001, in a written or electronic format. Format for submitting the VSP electronically can be found at <http://www.uscg.mil/HQ/MSC>.

(c) The VSP is sensitive security information and must be protected in accordance with 49 CFR part 1520.

(d) If the VSP is kept in an electronic format, procedures must be in place to prevent its unauthorized deletion, destruction, or amendment.